What is claimed is:

1. In a computing environment having a connection to a network, a computer program product for securely propagating security credentials from a trusted master registry, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for establishing a secure connection between a client and a password synchronization agent (PSA);

computer-readable program code means for transmitting an identifier of a user and an identifying secret of the user to the PSA;

computer-readable program code means for validating the user with the trusted master registry using the transmitted user identifier and identifying secret; and

computer-readable program code means for propagating the identifying secret of the user to one or more target registries if the validation succeeds.

2. The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing a second secure connection between the PSA and the trusted master registry; and

computer-readable program code means for using the second secure connection for the validating of the user.

3. The computer program product according to Claim 1, further comprising:

computer-readable program code means for establishing additional secure connections

between the PSA and each of the target registries; and

computer-readable program code means for using the additional secure connections for the propagating of the identifying secret.

4. The computer program product according to Claim 1, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret further comprises computer-readable program code means for identifying the target repositories using the stored password synchronization policy information for the user.

5. The computer program product according to Claim 1, wherein the master registry stores password synchronization policy information, and wherein the computer-readable program code means for propagating the identifying secret further comprises computer-readable program code means for identifying the target repositories using the stored password synchronization policy information for a user group of which the user is a member.

6. The computer program product according to Claim 1, wherein the computer-readable program code means for establishing the secure connection further comprises computer-readable program code means for authenticating the PSA to the client.

7. The computer program product according to Claim 2, wherein the computer-readable

program code means for establishing the second secure connection further comprises computer-readable program code means for authenticating the master registry to the PSA.

8. The computer program product according to Claim 3, wherein the computer-readable program code means for establishing additional secure connections further comprises computer-readable program code means for authenticating the one or more target registries to the PSA.

9. The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises:

computer-readable program code means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

computer-readable program code means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

computer-readable program code means for comparing the located identifying secret to a result of performing the security function.

10. The computer program product according to Claim 1, wherein the computer-readable program code means for validating further comprises computer-readable program code means for invoking an authenticated LDAP bind or other native authentication mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the

master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

11. The computer program product according to Claim 1, wherein the PSA has administrative authority for performing operations at the one or more target registries.

12. The computer program product according to Claim 1, further comprising:

computer-readable program code means for obtaining a new value from the user to be used as the propagated identifying secret; and

computer-readable program code means for substituting this new value for the identifying secret prior to operation of the computer-readable program code means for propagating.

13. A system for securely propagating security credentials from a trusted master registry, comprising:

means for establishing a secure connection between a client and a password synchronization agent (PSA);

means for transmitting an identifier of a user and an identifying secret of the user to the PSA;

means for validating the user with the trusted master registry using the transmitted user identifier and identifying secret; and

means for propagating the identifying secret of the user to one or more target repositories

the validation succeeds.

14. The system according to Claim 13, further comprising:

means for establishing a second secure connection between the PSA and the trusted master registry; and

means for using the second secure connection for the validating of the user.

15. The system according to Claim 13, further comprising:

means for establishing additional secure connections between the PSA and each of the target registries; and

means for using the additional secure connections for the propagating of the identifying secret.

16. The system according to Claim 13, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret further comprises means for identifying the target registries using the stored password synchronization policy information for the user.

17. The system according to Claim 13, wherein the master registry stores password synchronization policy information, and wherein the means for propagating the identifying secret further comprises means for identifying the target repositories using the stored password

synchronization policy information for a user group of which the user is a member.

18. The system according to Claim 13, wherein the means for establishing the secure connection further comprises means for authenticating the PSA to the client.

19. The system according to Claim 14, wherein the means for establishing the second secure connection further comprises means for authenticating the master registry to the PSA.

20. The system according to Claim 15, wherein the means for establishing additional secure connections further comprises means for authenticating the one or more target registries to the PSA.

21. The system according to Claim 13, wherein the means for validating further comprises:

means for performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

means for using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

means for comparing the located identifying secret to a result of performing the security function.

22. The system according to Claim 13, wherein the means for validating further comprises means for invoking an authenticated LDAP bind or other native authentication mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

23. The system according to Claim 13, wherein the PSA has administrative authority for performing operations at the one or more target registries.

24. The system according to Claim 13, further comprising:

means for obtaining a new value from the user to be used as the propagated identifying secret; and

means for substituting this new value for the identifying secret prior to operation of the means for propagating.

25. A method for securely propagating security credentials from a trusted master registry, comprising steps of:

establishing a secure connection between a client and a password synchronization agent (PSA);

transmitting an identifier of a user and an identifying secret of the user to the PSA;

validating the user with the trusted master registry using the transmitted user identifier and

identifying secret; and

propagating the identifying secret of the user to one or more target registries if the validation succeeds.

26. The method according to Claim 25, further comprising steps of:

establishing a second secure connection between the PSA and the trusted master registry; and

using the second secure connection for the validating of the user.

27. The method according to Claim 25, further comprising steps of:

establishing additional secure connections between the PSA and each of the target registries; and

using the additional secure connections for the propagating of the identifying secret.

28. The method according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the step of propagating the identifying secret further comprises the step of identifying the target registries using the stored password synchronization policy information for the user.

29. The method according to Claim 25, wherein the master registry stores password synchronization policy information, and wherein the step of propagating the identifying secret

further comprises the step of identifying the target registries using the stored password synchronization policy information for a user group of which the user is a member.

30. The method according to Claim 25, wherein the step of establishing the secure connection further comprises the step of authenticating the PSA to the client.

31. The method according to Claim 26, wherein the step of establishing the second secure connection further comprises the step of authenticating the master registry to the PSA.

32. The method according to Claim 27, wherein the step of establishing additional secure connections further comprises the step of authenticating the one or more target registries to the PSA.

33. The method according to Claim 25, wherein the step of validating further comprises:

performing a security function on the identifying secret of the user, wherein the security function comprises one of (i) a one-way hashing algorithm or (ii) an encryption algorithm;

using the user identifier to locate a previously-stored identifying secret of the user which was stored by the master registry; and

comparing the located identifying secret to a result of performing the security function.

34. The method according to Claim 25, wherein the step of validating further comprises the

step of invoking an authenticated LDAP bind or other native authentication mechanism of the master registry, wherein the identifier of the user and the identifying secret of the user are passed to the master registry, thereby causing the master registry to validate the passed identifier and identifying secret and return a result which reports a success or failure of the validation.

35. The method according to Claim 25, wherein the PSA has administrative authority for performing operations at the one or more target registries.

36. The method according to Claim 25, further comprising steps of:

obtaining a new value from the user to be used as the propagated identifying secret; and

substituting this new value for the identifying secret prior to operation of the propagating step.